KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma / Tietoverkkotekniikka

Joni Korjala

TIETOTURVAKATSAUKSEN TOTEUTUS TIETOTURVA-AUDITOINNIN JA PENETRAATIOTESTAUKSEN MENETELMIÄ HYÖDYNTÄEN

Opinnäytetyö 2014

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma

KORJALA, JONI	Tietoturvakatsauksen toteutus tietoturva-auditoinnin ja penetraatiotestauksen menetelmiä hyödyntäen
Opinnäytetyö	32 sivua
Työn ohjaaja	Martti Kettunen, yliopettaja
Toimeksiantaja	Kymenlaakson ammattikorkeakoulu
Huhtikuu 2014	
Avainsanat	tietoturva-auditointi, penetraatiotestaus, tietoturva

Tietojen varastaminen ja erilaiset tietoverkkorikokset ovat yleistyneet viime vuosien aikana huomattavasti, ja saammekin kuulla niistä lähes päivittäin mediassa. Näin ollen tietoturvallisuustyön merkitys korostuu entisestään ja osaamiselle on tarvetta.

Tämän opinnäytetyön tavoitteena oli toteuttaa Kymenlaakson ammattikorkeakoulun tietotekniikan koulutusohjelman ICT-LAB tuotantoympäristöön tietoturvakatsaus, jossa yritettiin löytää mahdollisimman paljon haavoittuvuuksia ja puutteita tietoturvan osalta hyödyntäen tietoturva-auditoinnin ja penetraatiotestauksen menetelmiä. Tietoturvakatsaus perustuu auditoijan osaamiseen ja mielipiteeseen, eikä siinä käytetä hyväksi mitään tietoturvastandardia tai viitekehystä.

Opinnäytetyössä perehdyttiin teoriaan alan kirjallisuutta apuna käyttäen ja käytettiin hyväksi koulutuksen tarjoamaa aiempaa osaamista. Opinnäytetyön käytännön vaiheessa toteutettiin erilaisia testejä ja tutkittiin saatavilla olevia dokumentaatioita toimeksiantajan ICT-LAB-tuotantoympäristöstä.

Tuloksena syntyi pohjatietoa tietoturvapuutteista ja haavoittuvuuksista tietoturvan eri osa-alueilta, ja tulosten perusteella toimeksiantaja on aloittanut tietoturvan parantamisen ICT-LAB-tuotantoympäristössään. Penetraatiotestauksessa ei ehditty hyväksikäyttämisvaiheeseen ajan loppuessa kesken.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Information Technology

KORJALA, JONI	Implementing the Security Review Utilizing the Methods of Security Auditing and Penetration Testing
Bachelor's Thesis	32 pages
Supervisor	Martti Kettunen, Principal Lecturer
Commissioned by	Kymenlaakso University of Applied Sciences
April 2014	
Keywords	security auditing, penetration testing, information security

Stealing confidential data and other cyber crimes are increasing problems which can be read about every day from media. This leads to the fact that the meaning of security process and maintaining system is emphasized and there is a need for professionals to solve the problems.

The main objective of this thesis was to implement the Security Review to ICT-LAB production network of Information Technology program at Kymenlaakso University of Applied Sciences. In the Security Review the issues and vulnerabilities were tried to be examined as much as possible utilizing the methods of security auditing and penetration testing. The Security Review was based on the auditor´s experience. However, in the Security Review no Security Standard or Framework was used.

In this study the theoretical framework consisted of the literature and the previous knowing based on the education. In the empirical phase of the study different tests and reviews were implemented and available documentations from the ICT-LAB production network of Kyamk was searched.

As a result, issues and vulnerabilities from different fields of information security were found and Kyamk has begun some improvements in the ICT-LAB production network based on the results. On the other hand, the exploitation phase of the penetration testing was not accomplished because the time ran out.

SISÄLLYS

LYHENTEET JA TERMIT

COBIT	Control Objectives for Information and Related Technology *eli viitekehys information ja teknologian hallinnointiin ja johtamiseen*
DMZ	Demilitarized Zone *eli deliminiratisoitu alue*
HTTP	Hypertext Transfer Protocol *eli hypertekstin siirtoprotokolla*
HTTPS	Hypertext Transfer Protocol Secure *eli suojattu hypertekstin siirtoprotokolla*
NIST	The National Institute of Standards and Testing *eli standardeja ja tekniikoita kehittävä Yhdysvaltojen kauppaministeriön virasto*
IDS	Intrusion Detection System *eli tunkeutumisenhavaitsemisjärjestelmä*
IPS	Intrusion Prevention System *eli tunkeutumisenestojärjestelmä*
IPv4	Internet Protocol version 4 *eli Internet-protokollan versio 4*
IPv6	Internet Protocol version 6 *eli Internet-protokollan versio 6*
ISMS	Information Security Management System *eli tietoturvan hallinnointiin käytettävä järjestelmä*
ISO 27000	*Tietoturvallisuuden hallintajärjestelmä*
LCCE	Learning and Competence Creating Ecosystem *eli Kymenlaakson ammattikorkeakoulun tavaramerkki, joka mahdollistaa välittömän yhteistyön korkeakoulun ja yritysten välillä.*

SNMP	Simple Network Management Protocol *eli TCP/IP-verkkojen hallintaprotokolla*
Telnet	*Yhteysprotokolla*
VPN	Virtual Private Network *eli virtuaalinen yksityisverkko*
WLAN	Wireless Local Area Network *eli langaton lähiverkko*

1 JOHDANTO

Nykyään tietojärjestelmät ovat hyvin haavoittuvaisia. Siitä hyvänä todisteena on, että jopa herkimmät ja vahvimmin suojatut järjestelmät joutuvat tunkeutumisen ja tiedon varastamisen uhreiksi. Hakkerointia on vaikea määritellä, mutta riski hakkeroiduksi tulemiselle on joka tapauksessa syvällä sivilisaatiomme kyberturvallisuusongelmien ytimessä. (Garfinkel 2012, 29.)

Suomen valtiovallalla on tärkeä tehtävä huolehtia kansalaisistaan kokonaisvaltaisesti eri voimavaroja laaja-alaisesti hyödyntäen. Yhtenä osana ihmisten ja koko yhteiskunnan huolehtimista on turvallisuudesta huolehtiminen, joka määritellään viranomaisten, järjestöjen ja elinkeinoelämän kanssa yhteistyössä sovitussa Yhteiskunnan turvallisuusstrategiassa 2010. Tämän strategian tavoitteena on turvata yhteiskunnan ja kansalaisten toimintakyky ja turvallisuus sekä säilyttää Suomen itsenäisyys. (Puolustusministeriö 2011, 1–3.) Yhtenä osana Yhteiskunnan turvallisuusstrategian toimeenpanoa on Suomen kyberturvallisuusstrategia, jonka tavoitteena on turvata kybertoimintaympäristö kaikissa mahdollisissa tilanteissa. Kybertoimintaympäristöllä tarkoitetaan sitä virtuaalista tieto- ja toimintaympäristöä, jossa myös Suomi tietoyhteiskuntana toimii päivittäin lukuisissa tilanteissa. Suomen kyberturvallisuusstrategiassa määritellään ne tavoitteet ja linjaukset, joiden perusteella tavoitellaan Suomen kybertoimintaympäristön turvallista toimivuutta ja haasteisiin vastaamista. (Turvallisuuskomitean sihteeristö 2013, 1–2, 6.)

Tulevaisuudessa kyberturvallisuus alana tulee työllistämään paljon, minkä seurauksena Kymenlaakson ammattikorkeakoulun (Kyamk) tietoverkkotekniikka on päättänyt vastata haasteeseen tarjoamalla opintokokonaisuuden kyberturvallisuudesta. Opintokokonaisuus koostuu tietoturvasta, tietoturvalaitteista ja hakkerointitekniikoista, joiden lisäksi voi valita vapaastivalittavan kyberturvallisuuden LCCE -projektin. (Kyamkin tietoverkkotekniikka 2013.)

Tämä opinnäytetyö on osa uutta Kymenlaakson ammattikorkeakoulun kyberturvallisuuslaboratoriohanketta, jonka pohjalta nousi tarve selvittää toimeksiantajan eli Kymenlaakson ammatikorkeakoulun tietotekniikan koulutusohjelman tuotantoympäristön mahdolliset tietoturvahaavoittuvuudet ja tietoturvaan liittyvät puutteet. Opinnäytetyön tarkoituksena onkin toteuttaa tietoturvakatsaus ICT-LAB:n tuotantoympäristöstä tietoturva-auditoinnin ja penetraatiotestauksen menetelmiä apuna käyttäen.

Tietoturvakatsauksen tarkoituksena on kartoittaa selvimmät ja silmäänpistävimmät aukot, riskit ja muut järjestelmän puutteet tietoturvaan liittyen. Katsaus onkin hyvä pohja laajemmalle auditoinnille, jota ei ole tämän opinnäytetyön puitteissa mahdollista toteuttaa. Näin ollen opinnäytetyön laajuuden ja siihen varatun ajan puitteissa katsaus vaikutti järkevimmältä vaihtoehdolta. Järjestelmää saadaan kuitenkin hyvin testattua käytännössä erilaisilla työkaluilla ja menetelmillä opinnäytetyön tavoitteen saavuttamiseksi.

2 TIETOTURVA-AUDITOINTI

Liiketoiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen jatkuvan toiminnan varmistaminen, tietojen ja järjestelmien luvattoman käytön estäminen, tahallisen ja tahattoman tiedon tuhoutumisen sekä vääristämisen estäminen ovat tietoturvallisuustyön turvaamisen päämääriä. Perinteisesti tietoturvallisuus jaetaan kahdeksaan eri osaan: hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus. (Andreasson & Koivisto 2013, 29, 52.)

Auditoinnit ja muu jatkuva seuranta kuuluvat tärkeimpiin huomioon otettaviin asioihin tietoturvan hallinnassa. Valvontaa ja tarvittaessa erityisiä auditoijia tulee käyttää antamaan lausuntoja sopimuskumppanien toiminnasta liittyen salaisen tiedon käsittelemiseen. (Andersson & Koivisto 2013, 51.) Tietoturva-auditoinnin tarkoitus on puolueettomasti testata, onko organisaation tietoturva riittävällä tasolla sen etuuksien suojaamisessa. Lisäksi sen on tarkoitus kertoa, mitä mahdollisia tietoturvan osa-alueita organisaation tulisi parantaa. Auditoinnin edetessä selvitetään organisaatioon kohdistuvat tietoturvariskit ja kuinka tietoturvariskeihin on varauduttu. (Jackson 2010, 20.)

2.1 Tietoturva-auditoinnin tyypit

Tietoturvakatsaus, tietoturva-arviointi ja tietoturva-auditointi ovat auditointityyppejä, jotka Chris Jackson on kirjoittanut kirjassaan *Network Security Auditing*. Auditoinnit voidaan siis jakaa tyyppeihin eri tavoin auditoinnin tarkoituksen, rajauksen ja tarkkuuden mukaan, mutta tyypit eivät silti poissulje toisiaan ja niitä voidaankin käyttää auditointiprosessin eri vaiheissa. (Jackson 2010, 19.)

Tietoturvakatsauksessa (*eng. Security Review*) pyritään kartoittamaan silmäänpistävimmät aukot, riskit ja ongelmat. Tietoturvakatsaus toimiikin hyvin pohjana varsinaiselle auditoinnille. Siinä käytetään hyväksi erilaisia työkaluja ja menetelmiä, esimerkiksi penetraatiotestausta tai haavoittuvuusskannausta. Se perustuu pitkälti auditoijan kokemukseen ja mielipiteeseen, jossa saadaan suurinpiirteinen tietoturvan tason kartoitus. (Jackson 2010, 19.)

Tietoturva-arvioinnissa (*eng. Security Assessment*) analysoidaan havaittuja riskejä ja puutteita sekä niiden kriittisyyttä organisaatiota kohtaan. Tietoturvakatsauksen tapaan tietoturva-arviointi perustuu pitkälti auditoijan kokemukseen ja mielipiteeseen. Tietoturva-arviointi antaa kuitenkin tarkemman kuvan, koska siinä puutteet on havainnoitu ja analysoitu. (Jackson 2010, 19.)

Tietoturva-auditointissa (*eng. Security Audit*) käytetään viitekehyksenä auditoijan ammattitaitoa ja jotain tietoturvastandardia tai ohjeistusta, joka pitää sisällään tietoturvakatsauksen sekä tietoturva-arvioinnin. Tietoturva-auditoinnin tuloksena määrittyy, kuinka hyvin organisaation tietoturvan taso vastaa standardin suosituksia. Auditoinnin aikana voidaan lisäksi selvittää, onko organisaation tietoturvapolitiikka ja sen prosessit viitekehyksen mukaisia, kuinka organisaatio on varautunut riskeihin sekä kuinka hyvin henkilöstö noudattaa sitä. (Jackson 2010, 20.)

2.2 Auditointiprosessi

Suunnitteluvaihe on auditointiprosessin ensimmäinen ja tärkein vaihe, jossa määritellään muun muassa käytetty strategia, auditoinnin kohde tai kohteet, käytettävät menetelmät ja työkalut sekä auditointiin sopiva viitekehys. Auditoinnissa voidaan esimerksi varmistaa, vastaako organisaation tietoturva standardia tai ohjeistusta, jota sen tulisi noudattaa. Suunnitteluvaiheeseen kerätään erilaista tietoa organisaatiosta, mietitään ketä henkilöistä ja mitä osastoja organisaatiosta aiotaan haastatella ja tarkastella. Aikataulun luominen on myös tärkeää auditoinnin onnistumisen kannalta. Lisäksi tulee sopia auditoitavan organisaation kanssa, milloin audiointi olisi hyvä suorittaa ja keitä auditoitavasta organisaatiosta tulisi olla paikalla. (Jackson 2010, 22.)

Kenttätutkimuksessa kerätään tietoa organisaatiosta suunnitelluista asioista. Voidaan esimerksi tarkastella järjestelmien dokumentaatioita, haastatella organisaation henkilökuntaa ja johtoa, tutkia aiempia auditointeja, järjestelmien lokitietoja ja raportteja

sekä konfiguraatioita. Jos kenttätutkimuksen aikana tulee ilmi kohteita tai asioita, joita ei ollut suunnitteluvaiheessa suunniteltu, tulee nekin silti ottaa huomioon koko auditoinnissa sen laadun varmistamiseksi. (Jackson 2010, 23–24.)

Analysointivaihe on auditoinnin seuraava vaihe, jossa kerätty aineisto analysoidaan. Siinä aineistoa luokitellaan ja analysoidaan ja sen perusteella havaitut tietoturvapuutteet järjestetään tärkeysjärjestetykseen suhteessa käytettyyn viitekehykseen ja suhteessa puutteiden kriittisyyteen. Auditoijan ammattitaito on tärkeässä roolissa analysointivaiheessa, koska sen perusteella havaitut tietoturvapuutteet järjestellään auditoinnin tarkoituksen mukaan. (Jackson 2010, 24.)

Tuloksista annetaan organisaatiolle yksityiskohtainen raportti, josta selviää, mitkä asiat ovat kriittisiä ja mitä niille kannattaisi tehdä tietoturvan parantamiseksi. Raportin lisäksi myös muu auditointiprosessin aikana dokumentoitu materiaali olisi hyvä antaa auditoidulle organisaatiolle, jotta se voisi jatkossa käyttää sitä esimerkiksi seuraavaa auditointia varten. (Jackson 2010, 24–25.)

Auditointiprosessin viimeisin vaihe on jälkitoimet. Siinä havaitut puutteet korjataan ja auditoidaan, jotta varmistutaan tietoturvan parantuneen. Puolueettomuuden säilyttämiseksi korjaustoimenpiteitä eivät suorita auditoijat itse. (Jackson 2010, 25.)

2.3 Viitekehykset ja standardit

Tietoturvan toteuttamiseen ja sen auditointiin on kehitetty erilaisia viitekehyksiä, standardeja ja ohjeistuksia. Viitekehykset kertovat, kuinka organisaatio voi hallinnoida tietoturvaa tehokkaasti. COBIT on eräs tunnettu viitekehys, jonka tarkoitus on auttaa organisaatiota hahmottamaan asiat ja toiminnot, joita sen tietojenkäsittely pitää sisällään. (Jackson 2010, 68.)

Tietoturvastandardit puolestaan kattavat tietoturvan toteuttamiseen käytettävät käytännöt tiedonkäsittelystä fyysiseen tietoturvallisuuten ja politiikkoihin. Standardit helpottavat auditoijaa erottamaan hyvän tietoturvan rakenteen huonosta. ISO 27000 sarja on ISMS-tietoturvajärjestelmän luomiseen ja käyttöön liittyvä kansainvälisesti tunnettu tietoturvakontrollien standardi. Se on yksi laajimmin käytetyistä ja viitatuista dokumenteista tietoturvan alalla nykyään. (Jackson 2010, 76.)

2.4 Tietoturva-auditoinnin kohteita

Riippuen auditoinnin tarkoituksesta, auditoijaa voidaan pyytää tutkimaan erilaisia järjestelmiä ja prosesseja. Tarkoituksen perusteella määrittyy auditoidaanko tietoturvapolitiikkaa, proseduuria vai hallintaa. Osa auditoinneista keskittyy vain tietoturvapolitiikkaan, kun taas osa ottaa huomioon kaikki kolme näkökulmaa. Voi olla vaikea rajata kategorioita toisistaan riippumatta siitä, kuinka yksityiskohtainen auditointi on. (Jackson 2010, 21.)

Henkilöstö, prosessit ja teknologia ovat tietoturvan hallinnan osa-alueita ja kaikkia niitä pystytään auditoimaan. Henkilöstön merkitys on suuri tietoturvan toteutumisen osalta organisaation jokapäiväisessä toiminnassa, sillä tietotekniikan rooli organisaatioissa laajenee ja tarvittavat tietoturvatoimenpiteet lisäävät tietämyksen tarvetta. Vaikka palkattaisiin henkilö vastamaan organisaation tietoturvasta, se ei millään riitä, jos organisaatiossa muut eivät tiedä omia vastuitaan tietoturvan toteutumisessa. Henkilöstön tulee olla tietoinen organisaation tietoturvapolitiikasta ja kuinka sitä noudatetaan. Riskejä voidaan hallita ja pienentää järjestämällä tietoturvakoulutuksia ja käyttämällä rangaistuksia tietoturvapolitiikan noudattamattomuudesta. (Jackson 2010, 5–6.)

Säännöllisellä järjestelmän auditoinnilla pyritään varmistamaan, että järjestelmä on pysynyt vaatimustenmukaisena. Auditointia on mahdollista suorittaa manuaalisesti, mutta on myös olemassa erilaisia automatisoituja työkaluja. On tärkeää paikallisen auditoinnin lisäksi auditoida järjestelmää myös tietoverkosta. Järjestelmän vaatimustenmukaisuutta pystytään valvomaan lähes reaaliajassa siihen tarkoitetulla työkalulla, joka antaa järjestelmän poikkeamista automaattisia raportteja. (Laaksonen, Nevasalo & Tomula 2006, 216.)

3 PENETRAATIOTESTAUS

On olemassa monenlaisia termejä kuvaamaan tietoturvallisuuden teknisen osan tarkastelua, esimerkkeinä eettinen hakkerointi, penetraatiotestaus ja haavoittuvuustestaus. Auditoijan pitäisi tietää perusteet testaustyökaluista ja tekniikoista. (Jackson 2010, 91–92.) Työssä kerrottujen menetelmien tarkoitus on tukea järjestelmän haavoittuvuuksien testausta, auttaa ymmärtämään mahdollisia uhkia ja suojautumaan saman-

tyyppisiltä uhilta. Eettisessä hakkeroinnissa pyritään ymmärtämään asiat hakkerin näkökulmasta, mutta taitoja käytetään hyvään tarkoitukseen. (Melnichuk 2008, 7.)

Haavoittuvuustestauksen ja penetraatiotestauksen ero on tärkeä ymmärtää ja joskus näitä termejä kuullaan käytettävän väärin. Haavoittuvuustestaus on prosessi, jossa tarkastellaan palveluiden ja järjestelmien potentiaalisia tietoturvapuutteita. Penetraatiotestauksessa puolestaan yritetään hyväksikäyttää haavoittuvuuksia simuloimalla hakkeria. Haavoittuvuustestauksen voi määrittää yhdeksi osaksi penetraatiotestausta. (Engebretson 2013, 1–2.)

Haavoittuvuus on johonkin asiaan liittyvä heikkous, joka mahdollistaa uhan toteutumisen. Vaikka sovellus- ja laitteistohaavoittuvuuksia havaintaankin lähes joka päivä, suurin osa haavoittuvuuksista edelleen johtuu järjestelmien vääränlaisesta konfiguraatiosta. Haavoittuvuustestauksen tarkoitus on selvittää mahdollisimman moni potentiaalinen järjestelmän heikkous. Nykypäivänä on saatavilla monenlaisia kaupallisia ja avoimeen lähdekoodin perustuvia työkaluja haavoittuvuustestaukseen. (Jackson 2010, 10, 91.)

Penetraatiotestauksen tarkoituksena on selvittää, miten testauksen kohteena olevassa verkossa on huolehdittu ennaltaehkäisystä, havaitsemisesta ja korjautuvuudesta yrittäen käyttää hyödyksi haavoittuvuuksia ja saada järjestelmät ja palvelut haltuun. Monet ammattilais-penetraatiotestaajat käyttävät sekä valmiita työkaluja että omia skriptauksiaan ja ohjelmiaan suorittaessaan penetraatiotestausta. (Jackson 2010, 116.)

3.1 Penetraatiotestauksen tyypit

Puhuttaessa penetraatiotestauksesta sen eri tyypit jaetaan sen mukaan, paljonko auditoija tai testaaja tietää järjestelmästä. Toisaalta auditoijat eivät mene penetraatiotestauksessaan samalle tasolle kuin hakkerit. Whitebox-testauksessa testaajalla on täydelliset tiedot järjestelmän rakenteesta, konfiguraatiosta, IP-osoitteista ja tarvittaessa myös lähdekoodista. Tätä tyyppiä käytetään yleensä simuloimaan pahinta mahdollista skenaariota hyökkääjän tietäessä perinpohjaisesti järjestelmän rakenteen. (Jackson 2010, 91–92.) Blackbox-testauksessa testaaja toisaalta simuloi ulkopuolista hakkeria, jolla ei ole tietoa järjestelmästä. Löydettyjä heikkouksia voidaan käyttää hyväksi julkisesti saatavilla tiedoilla. Graybox-testaus puolestaan sijoittuu johonkin Whitebox- ja Blackbox-testauksen väliin. Siinä testaajalle annetaan aluksi joitain tietoja järjestel-

mästä, joilla hän pääsee alkuun. Esimerkiksi simuloidessaan sisäistä hyökkääjää testaajalle tarjotaan IP-osoitteita ja käyttäjätason oikeudet järjestelmään. (Jackson 2010, 92.)

"Punaiset vastaan siniset" -asetelma tulee sotilasmaailmasta, jossa taistelevat joukkueet testaavat toistensa operatiivisia valmiuksia. Tietokonemaailmassa "punaiset vastaan siniset" on ikään kuin sotapeli, jossa organisaatiota testataan niin todellisen skenaarion muodossa kuin mahdollista. Punainen joukkue yrittää kaikin mahdollisin keinoin päästä tunkeutumaan sinisen joukkueen järjestelmään. Tämä arviointitapa testaa politiikan ja proseduurit, havaitsemisen, tapauksen käsittelyn, fyysisen turvallisuuden, turvallisuustietoisuuden ja muut alueet, joita voidaan käyttää hyväksi. (Jackson 2010, 92.)

3.2 Penetraatiotestauksen vaiheet

Penetraatiotestaus voidaan jakaa eri vaiheisiin ja vaiheiden määrä sekä vaiheiden nimitykset vaihtelevat kirjoittajasta riippuen. Riippumatta vaiheiden lukumäärästä ja vaiheiden nimityksistä, kaikista muodostuu kuitenkin perusajatus penetraatiotestauksesta. Penetraatiotestaus voidaan jakaa esimerkiksi tiedusteluun, skannaukseen, hyväksikäyttämiseen ja kaappauksen ylläpitämiseen. (Engerbretson 2013, 14.)

3.2.1 Tiedusteluvaihe

Penetraatiotestaus alkaa tiedusteluvaiheella (*eng. Reconnaissance*), mutta voidaan puhua myös tiedonkeruuvaiheesta (*eng. Information Gathering*), jossa valmistaudutaan penetraatiotestaukseen keräämällä erilaista tietoa testattavasta kohteesta. Mitä enemmän aikaa tiedon keräämiseen käytetään, sitä paremmat ovat mahdollisuudet myöhempien vaiheiden onnistumiselle. Esimerkiksi penetraatiotestaajalle voidaan antaa ainoastaan testattavan yrityksen nimi, jonka perusteella testaaja alkaa tutkia mahdollisuuksia tunkeutua yrityksen tietoverkkoon. (Engebretson 2013, 20–23.)

Tiedonkeruuta voidaan suorittaa passiivisesti tai aktiivisesti. Passiivisessa tiedonkeruussa tietoa yritetään saada kohteen tietoverkosta ja järjestelmästä ottamatta yhteyttä suoraan kohteeseen. Esimerkkejä passiivisen tiedonkeruun työkaluista ovat Internetselain, nslookup, archieve.org ja dig. Näillä työkaluilla voidaan saada kohteesta selville muun muassa web-palvelimien osoitteet, palvelimen tyypin, palvelimen sijainnin,

palvelimen hakemistojuuren, käytetyn teknologian (ohjelmisto/hardware), salaus standardin, lomakkeiden kentät, yrityksen yhteystiedot ja metatietoja. (Wilhelm 2013, 151–158.)

Aktiivisessa tiedonkeruussa puolestaan otetaan yhteyttä suoraan kohteeseen ja siinä voidaan varmistaa passiivisesti kerättyjä tietoja todeksi. Yksi todella tehokas tiedonkeruu metodi on Social Engineering. (Wilhelm 2013, 172.) Hyvä esimerkki Social Engineeringstä on, että esitetään puhelimessa yrityksen IT-vastaavaa ja tiedustellaa yrityksen työntekijältä käyttäjätunnuksia ja salasanoja (Melnichuk 2008, 47).

3.2.2 Skannausvaihe

Tiedonkeruun jälkeen siirrytään skannausvaiheeseen (*eng. Scanning*), jolloin penetraatiotestaajalla pitäisi olla ymmärrys kohteesta ja yksityiskohtaista kerättyä tietoa, toisin sanoen kohteelle kuuluvia IP-osoitteita. Vaiheesta puhutaan myös nimellä haavoittuvuustunnistus (*eng. Vulnerability Identification*). Skannausvaiheessa varmistetaan luetellussa järjestyksessä, onko kohdejärjestelmä elossa ja kykeneväinen kommunikoimaan penetraatiotestaajan kanssa, selvitetään avoimet portit ja palvelut porttiskannauksella ja suoritetaan haavoittuvuus-skannausta. (Engebretson 2013, 53–55.)

Valmiit skannausohjelmat saattavat havaita satoja sivuja haavoittuvuuksia, joita ei kuitenkaan tosi elämässä pystyisi käyttämään hyväksi. Työkalut soveltuvat hyvin auditoijan avuksi havaitsemaan heikkouksia. (Jackson 2010, 101.) Esimerkiksi Nessus on suosittu haavoittuvuuksien havaitsemiseen käytettävä ohjelma. Se etsii tunnettuja haavoittuvuuksia käyttöjärjestelmistä, tietoverkoista ja sovelluksista. Nessus on saatavilla Windowsille, Linuxille ja Max OS X:lle. Nessus on kaupallinen ohjelma, mutta siitä on saatavilla 7-päivän kokeiluversio rajoitetuin ominaisuuksin.

3.2.2.1 Nmap

Nmap on ilmainen ja avoimeen lähdekoodiin perustuva tietoverkon havainnointiin ja tietoturva-auditointiin käytettävä työkalu. Se on saatavilla yleisimpiin käyttöjärjestelmiin, ja komentoriviin perustuvan version lisäksi Nmapiin saa myös graafisia käyttöliittymiä. (Pale 2012, 10.) Auditoijat voivat käyttää sitä esimerkiksi saamaan käsityksen siitä, mitä isäntäpalvelimia ja palveluita on saatavilla verkossa (Jackson 2010, 96). Nmap käyttää muokkaamattomia IP-paketteja määrittämään isäntien saatavuttaa ver-

kosta, selvittämään mitä käyttöjärjestelmää ja versiota ne käyttävät, minkä tyyppisiä pakettien suodatuksia tai palomuureja niillä on käytössä sekä tusinoittain muita ominaisuuksia. Nmap on olennainen työkalu kaikille tietoturva-ammattilaisille ja verkon ylläpitäjille turvallisuuden arvioinnassa, monitoroinnissa ja tehokkaassa hallinnoinnissa. (Pale 2012, 10.)

Nmapin suosituin ominaisuus on palvelun version selvittäminen. Palvelun tarkan version tuntemus on tärkeää penetraatiotestaajille, jotka etsivät palveluiden haavoittuvuuksia sekä järjestelmävastaaville, jotka monitoroivat verkon luvattomia muutoksia. (Pale 2012, 20.) Esimerkiksi seuraavanlaisella komennolla saadaan vastaus kohteen palveluista ja versioista:

nmap -sV localhost

Vaihtoehtoisesti agressiivisemmin voi hankkia tietoa komennolla:

nmap -A localhost

Nämä komennot toimivat IPv4-osoitteisiin isäntiin. Nmapista löytyy tuki myös IPv6-osoitteiden käyttämiseen. Avoimet portit ja palveluiden versiot saadaan selville komennolla:

nmap -6 ::1

3.2.3 Haavoittuvuuden hyväksikäyttäminen

Kohteen käyttämien ohjelmien, palveluiden ja niiden versioiden selvittämisen jälkeen penetraatiotestaaja alkaa etsiä, löytyisikö ohjelmasta haavoittuvuuksia, joita voisi käyttää hyväksi esimerkiksi Exploit-DB (www.exploit-db.com) tai NIST National Vulnerability Databasesta. Haavoittuvuuden hyväksikäyttämisvaiheessa (*eng. Vulnerability Exploitation*) järjestelmään yritetään siis tunkeutua luvattomasti sisään hyödyntämällä jonkin kohteen käyttämän ohjelman version haavoittuvuutta. Tärkeää on kuitenkin ymmärtää, että järjestelmää ei aina saada kaikilla haavoittuvuuksilla täyteen hallintaan. (Wilhelm 2013, 211–213.)

Exploit on esimerkiksi pala ohjelmakoodia tai skripti, jolla pystytään käyttämään hyväksi jotakin tiettyä haavoittuvuutta. Paikallisen exploitin (*eng. Local Exploit*) suorittamiseen tarvitaan pääsy ja oikeudet koneeseen. Yleensä näitä käytetään korottamaan oikeudet tavallisesta käyttäjästä adminiksi tai rootiksi, toisin sanoen saamaan paremmat oikeudet isäntäkoneeseen. Etä-exploitin (*eng. Remote Exploit*) tarkoitus on lähes sama kuin paikallisen exploitin, mutta se voidaan suorittaa mistä vain Internetistä. (Melnichuk 2008, 59.)

Nollapäivä-haavoittuvuus (*eng. 0-day*) tarkoittaa, että haavoittuvuutta ei ole vielä havaittu, eikä siihen ole saatavilla korjaavia toimenpiteitä. Nämä haavoittuvuudet ovat yleensä vain hakkeriyhteisöjen tiedossa ja ovat "kovaa valuuttaa". Osa hakkereista tekeekin kauppaa löytämillään 0-day haavoittuvuuksilla. (Melnichuk 2008, 58.)

3.2.3.1 Metasploit

Järjestelmän haltuun ottamiseen on olemassa monia erilaisia automatisoituja työkaluja, esimerkkinä Metasploit. Se on tehokas, mukautuva ja ilmainen. Se sisältää sarjan erilaisia työkaluja, jotka puolestaan pitävät sisällään kymmeniä eri ominaisuuksia tarpeen mukaan. (Engebretson 2013, 85.)

Metasploit mahdollistaa erilaisten hyötykuormien (*eng. Payload*) käytön kohteeseen. Hyötykuormat ovat keskenään vaihtokelpoisia ja niitä ei ole sidottu tiettyyn exploittiin. Suosituimpia käytettyjä hyötykuormia ovat uusien käyttäjien lisäys, avoimet takaportit ja uuden ohjelman asentaminen kohteeseen. (Engebretson 2013, 85–86.)

3.2.4 Kaappauksen ylläpitäminen

Penetraatiotestauksen kohteena olevan kanssa on tärkeä keskustella ja selvittää tämä vaihe, jossa kaapattuun järjestelmään yritetään tehdä esimerkiksi takaovi (*eng. Backdoor*). Nykyään hyökkääjät ovat kiinnostuneita pitkäaikaisesta pääsystä kaapattuun järjestelmään verrattuna tilanteeseen vuosia taaksepäin, jolloin järjestelmään hakkeroiduttiin, varastettiin tietoja ja kadottiin sen jälkeen. (Engebretson 2013, 167–168.)

Takaovi on yksinkertaisimmillaan pala ohjelmakoodia, joka mahdollistaa hyökkääjän yhdistäytymisen uudelleen kohteeseen. Yleensä takaovi on naamioitu prosessiksi, joka

on käynnissä kohteessa ja sallii luvattoman käyttäjän hallita tietokonetta. (Engebretson 2013, 168.)

4 SUUNNITTELU JA TOTEUTUS

Opinnäytetyöni aihe sai alkunsa syksyllä 2013, kun tietoverkkotekniikan tiimivastaava antoi erään kotkalaisen yrityksen toimeksiannon minulle. Aihe ei kuitenkaan koskaan edennyt toimeksiantoa pidemmälle, koska kyseiseltä yritykseltä puuttui siihen resurssit. Sen seurauksena tiimivastaava ehdotti minulle uutta toimeksiantoa 12.11.2013 Kymenlaakson ammattikorkeakoulun puolesta samasta aihepiiristä, ainoastaan opinnäytetyöni kohde vaihtui ensimmäiseen toimeksiantoon nähden. Opinnäytetyöni aihe rajautui sen ennalta asetettujen tavoitteiden mukaisesti tarpeesta selvittää Kymenlaakson ammattikorkeakoulun ICT-LAB:n tuotantoympäristön haavoittuvuudet ja puutteet tietoturvaan liittyen.

Opinnäytetyöni aiheen rajauksen jälkeen aloitin syksyllä 2013 opinnäytetyöni tekemisen etsimällä aiempia tutkimuksia ja lähdekirjallisuutta. Hain monipuolisesti tietoa eri sähköisistä tietokannoista, korkeakoulujen Internet-sivuilta ja manuaalisesti Kotkan kaupungin pääkirjastosta ja Kymenlaakson ammattikorkeakoulun Metsolan kampuksen kirjastosta. Lisäksi käytin apunani Googlen vapaasanahakua kartoittamaan mahdollisia muita hyviä lähteitä.

Käytin sähköisinä tietokantoina Ebscoa ja Nelliä, joista etsin sopivia lähteitä hakusanoilla securit* audit*, penetration test*, pen* test*, hack*, ethical hack*, vulnerabili*, tietoturva* auditoin*, hakker*. Rajasin hakutulokset julkaisuajankohdan mukaan siten, että suljin hakutulosten ulkopuolelle yli viisi vuotta vanhat lähteet. Korkeakoulujen Internet-sivuilta en löytänyt opinnäytetyössäni hyödynnettäväksi kelpaavia lähteitä. Lisäksi etsin lähdekirjallisuutta edellämainitsemistani kirjastoista, mutta aihepiiriin liittyviä kirjoja ei ollut saatavilla. Googlen vapaasanahakua hyödyntämällä löysin hyvää ja aiheeseen sopivaa kirjallisuutta. Kirjastoista ei kuitenkaan löytynyt kyseisiä kirjoja, joten päätin tilata löytämäni kirjat verkkokaupoista. Huomionarvoisena mainittakoon, että suomenkielistä lähdemateriaalia ei juuri löytynyt, vaan suurin osa aiheeseeni liittyvästä materiaalista on englanninkielistä. Huomattuani heikon suomenkielisen materiaalin saatavuuden päädyin käyttämään englanninkielisiä hakusanoja. Etsin myös samankaltaisia opinnäytetöitä Theseus-tietokantaa apuna käyttäen, mutta niitä ei juuri löytynyt.

Talvella 2013–2014 opinnäytetyönsopimuksen kirjoittamisen jälkeen aloin teoria-osuuden kirjoittamisen ohella suunnitella opinnäytetyöni toteutusta. Koulutusohjelmavastaavamme tiedusteli halukkuuttani osallistua 9. – 10.1.2014 Clarified Securityn järjestämälle Hands on hacking -kurssille, joka on suunnatta järjestelmäasiantuntijoille, järjestelmävastaaville ja muille tietotekniikan parissa työskenteleville. Pidin ajatusta erinomaisena ja päätin osallistua kurssille, jonka sisältöön kuului teoriaa ja käytännön läheisiä harjoituksia penetraatiotestauksesta ja hakkeroinnista virtualisoidussa ympäristössä. Kurssin ansiosta opin omaksumaan hakkerien käyttämää ajatusmallia, josta oli minulle hyötyä opinnäytetyöni käytännönosuuden toteutuksessa. Lisätietoa kurssista on saatavilla Clarified Securityn Internet-sivuilta osoitteesta http://www.clarifiedsecurity.com/trainings/#hohe.

Kurssilta ja kirjallisuudesta saamani opin perusteella aloin suunnitella opinnäytetyöni käytännön osuuteen kuuluvan tietoturvakatsauksen suunnitelmaa, johon sisältyy kohteiden määrittely, käytettävät työkalut ja menetelmät sekä havainnointien dokumentointi ja raportointi toimeksiantajalle. Ennen tietoturvakatsauksen toteuttamista asensin auditoinnissa käytettävän tietokoneen.

4.1 ICT-LAB-tuotantoverkko

ICT-LAB on oppimisympäristö Kymenlaakson ammattikorkeakoulun tietotekniikan opiskelijoille. Siihen sisältyvät Cisco-lab ja SimuNet-lab, joita hyödynnetään tietoverkkotekniikan opinnoissa. ICT-LAB:n oppimisympäristön tietoverkkopalvelut tarjoaa Kalaverkoksi kutsuttu tuotantoverkko. Opinnäytetyöni käytännön osuus toteutetaan siis Kalaverkkoon, mutta selvyyden vuoksi puhun opinnäytetyössäni ICT-LAB-tuotantoverkosta.

Tuotantoverkko koostuu kahdesta L3-kytkimestä, kuudesta L2-kytkimestä, useammasta WLAN-tukiasemasta, kahdesta palomuurista IPv4 ja IPv6 liikenteelle, kymmenistä palvelimista, levyjärjestelmästä, valvontakameroista, tulostimista ja useammasta kymmenestä työasemasta. Verkon aktiivilaitteet ovat Ciscon tuotteita lukuunottamatta yhtä Dellin valmistamaa laitetta. Palvelimet ovat eri Linux- ja Windows-käyttöjärjestelmiä redundanttisella VMware-virtualisointialustalla.

4.2 Tietoturvakartoituksen suunnittelu

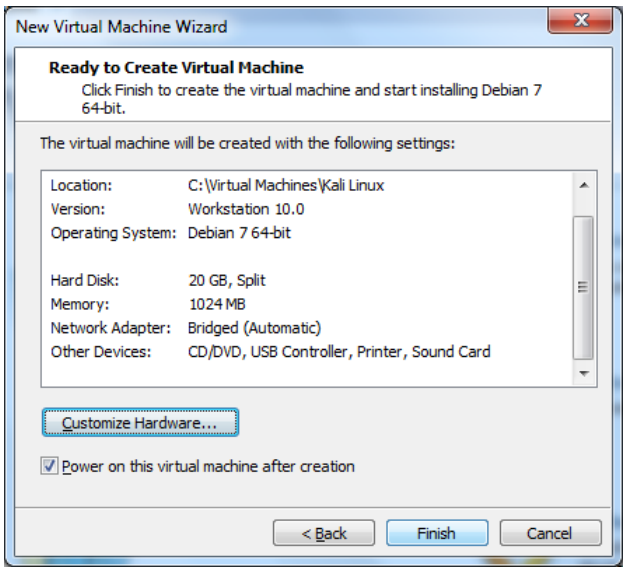
Tietoturvakartoituksen kohteena on Kymenlaakson ammattikorkeakoulun tietotekniikankoulutusohjelman ICT-LAB tuotantoympäristö. Kartoituksessa yritetään etsiä mahdollisimman paljon erilaisia haavoittuvuuksia, aukkoja, puutteita ja tietoturvariskejä tuotantoympäristön järjestelmistä ja laitteista. Tavoitteena on saada mahdollisimman laaja pohjakäsitys laboratorion tuotantoverkon tietoturvan tasosta ulkoverkosta hyökkäävään hakkerin näkökulmasta ja yleisesti tietoturvan ratkaisuista. Lisäksi tavoitteeni on saada lähtökohta siihen, mistä laboratorion tuotantoverkon tietoturvaa aletaan parantaa.

Tietoturvakartoitus kohdistetaan teknologiaan ja siinä pyritään käymään läpi tietoverkon aktiivilaitteet, palvelimet sekä mahdolliset muut laitteet, jotka ovat verkkoon kytkettynä. Ajan ollessa rajallinen pyritään etsimään ne silmäänpistävimmät haavoittuvuudet ja riskit, jotka tulisi korjata mahdollisimman pikaisesti. Tietoturvakartoituksen tekijä käy läpi erilaisia dokumentaatioita toimeksiantajan tietoverkosta ja tekee myös niiden pohjalta päätelmiä. Tekijä haastattelee myös tarpeen tullen toimeksiantajan henkilökuntaa.

Tietoturvakartoitus toteutetaan hyvin pitkälti opinnäytetyön tekijän resurssien ja osaamisen mukaan. Tekijä hankkii itse käyttämänsä työkalut ja hyödyntää koulutuksen aikana saamaa osaamistaan. Ajan ja opinnäytetyön laajuuden puitteissa tässä katsauksessa ei käytetä avuksi mitään tietoturvastandardia tai ohjeistusta. Tietoturvakartoituksen aikana tekijä käy läpi suunnitellut kohteensa ja käy tarvittaessa läpi myös ylimääräisiä kohteita, joita ei huomioitu suunnitteluvaiheessa. Tekijä tekee myös selvityksen toimeksiantajalle löytyneistä riskeistä.

4.3 Auditointikoneen toteutus

Päätin asentaa Kali Linux käyttöjärjestelmän virtuaalikoneeksi Windows 7 isäntäkoneeseen hyödyntäen VMware Workstation 10 -virtualisointiohjelmaa. Tämä oli järkevin vaihtoehto, koska koulutusohjelmamme tarjoaa opiskelijoilleen kannettavat tietokoneet ja opiskelijoilla on oikeus asentaa VMwaren tuotteita kahden vuoden lisenssillä. Näin saatiin tehtyä helposti tietokone opinnäytetyön tarkoituksiin.



Kuva 1. Virtuaalikoneen asetukset.

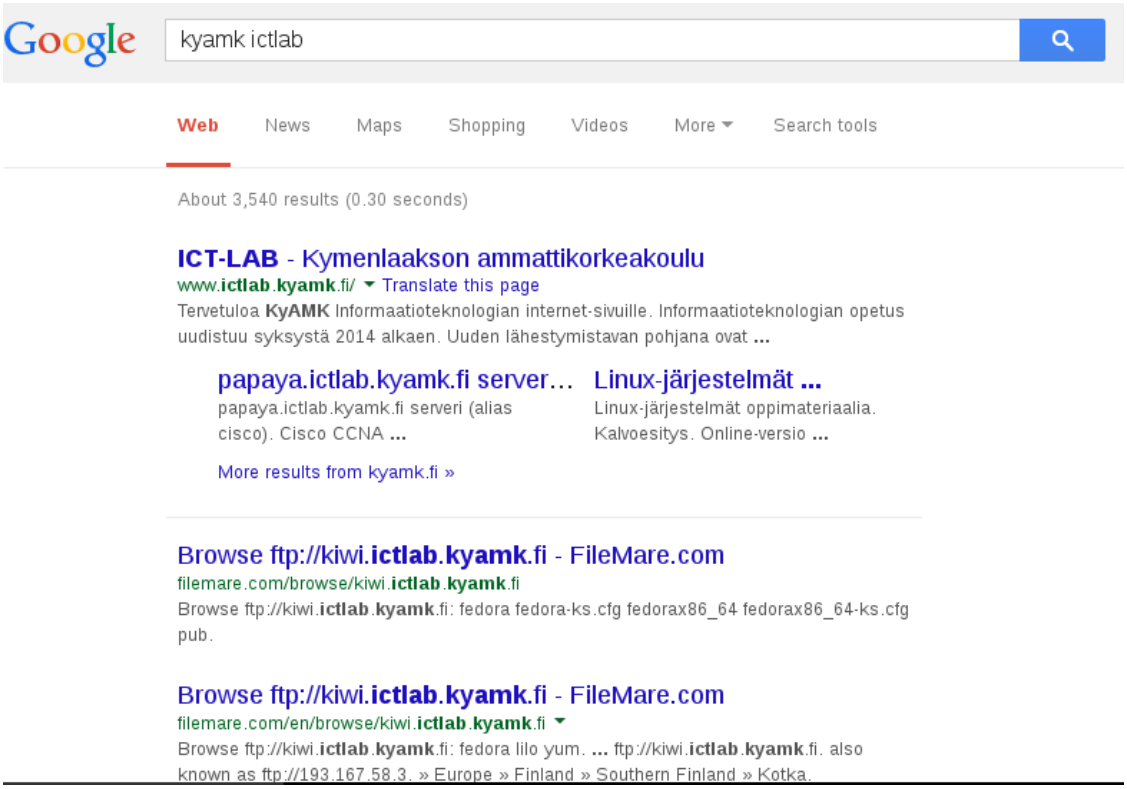
4.3.1 Kali Linux

Kali Linux on ilmainen tietoturva-auditointiin ja penetraatiotestaukseen käytettävä Linux-jakelu. Se on täysin uudistettu aiemmasta BackTrack Linuxista. Kali sisältää yli 300 penetraatiotestaukseen käytettävää työkalua. Sen lähdekoodi on täysin avoin ja kaikki koodi on saatavilla. (What is Kali Linux ? 2013.)

Kali on tuettu i386-, amd64- ja ARM-alustoille. Vähimmäisvaatimus kiintolevytilalle on 10 GB ja keskusmuistin määrälle 512 MB. Asennuksen voi toteuttaa CD-DVD-asemalla tai USB-bootilla, ja tarjolla on myös tarvittaessa verkkoasennus. (Kali Linux Hard Disk Install 2013.)

4.4 Tietoturvakatsauksen toteutus

Tietoturvakatsauksen toteuttamisen aloitin tutkimalla ICT-LAB-tuotantoympäristön laitekantaa ja osoitteistoa saatavilla olevista dokumentaatioista ja tallennetuista konfiguraatioista. Yritin saada mahdollisimman hyvän kuvan siitä, mistä tietoturvakatsauksen kohde koostuu. Samalla aloitin myös penetraatiotestauksen yrittämällä etsiä mahdollisimman paljon tietoa ainoastaa käyttämällä Kyamk- ja ICT-LAB-sanoja. Aluksi käytin Googlen vapaa-sanahakua.



Kuva 2. Vapaa-sanahaun tuottamia tuloksia.

Jatkoin tiedon hankintaa hyödyntämällä Archive.org -palvelua, jolla pystyy tarkastelemaan useamman vuoden takaisia versioita haluamastaan sivustosta. Halusin löytää myös muutakin tietoa kohteesta ja hyödynsin Netcraft.com -palvelua, joka listaa alidomaineja.

Network

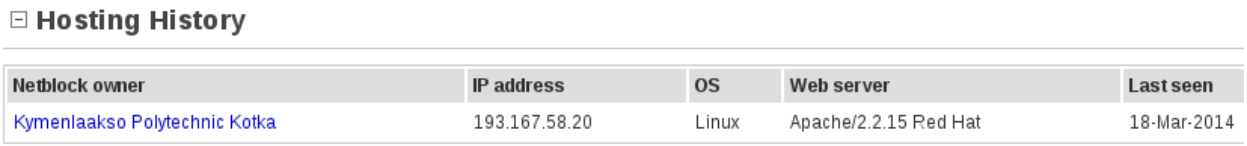
Site	http://www.ictlab.kyamk.fi	**Netblock Owner**	Kymenlaakso Polytechnic
Domain	kyamk.fi	**Nameserver**	ns.kyamk.fi
IP address	193.167.61.194	**DNS admin**	root@kyamk.fi
IPv6 address	*Not Present*	**Reverse DNS**	fws194.kyamk.fi
Domain registrar	ficora.fi	**Nameserver organisation**	whois.ficora.fi
Organisation	Kymenlaakson ammattikorkeakoulu oy, 10397304, Pasi ��p�l� / Tietohallinto, Pl 9, Kotka, 48401, Finland	**Hosting company**	kyamk.fi
Top Level Domain	Finland (.fi)	**DNS Security Extensions**	*unknown*
Hosting country	FI		

Hosting History

Netblock owner	IP address	OS	Web server
Kymenlaakso Polytechnic Kotka	193.167.61.194	Linux	Apache/2.2.15 Red Hat

Kuva 3. Netcraft.com -palvelun tarjoamia tietoja.

Google ehdotti aiemmin lisäksi osoitetta papaya.ictlab.kyamk.fi, joka liittyy Kyamkin tietoverkkotekniikan opetuslaboratorioon, josta päätinkin lisäksi hakea lisää tietoa Netcraft.com -palvelun avulla.



Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Kymenlaakso Polytechnic Kotka	193.167.58.20	Linux	Apache/2.2.15 Red Hat	18-Mar-2014

Kuva 4. Netcraft.com -palvelun tarjoamaa tietoa osoitteesta papaya.ictlab.kyamk.fi.

Tämän työkalun avulla sain selvitettyä jonkin mahdollisen IP-osoitteen ICT-LABin tuotantoympäristöstä. Tiedon keruuta todellisessa penetraatiotestauksessa olisi pitänyt jatkaa vielä ja hyödyntää erilaisia työkaluja, mutta opinnäytetyön laajuuden puitteissa penetraatiotestauksen tiedonkeruuvaihe päätettiin tähän.

IP-osoitteiden perusteella aloin kartoittaa kohteiden käyttöjärjestelmäversioita ja asennettuja ohjelmia sekä niiden versioita. Käytin esimerkiksi Nmap-työkalua, jolla sain listattua ohjelmien versioita seuraavalla komennolla:

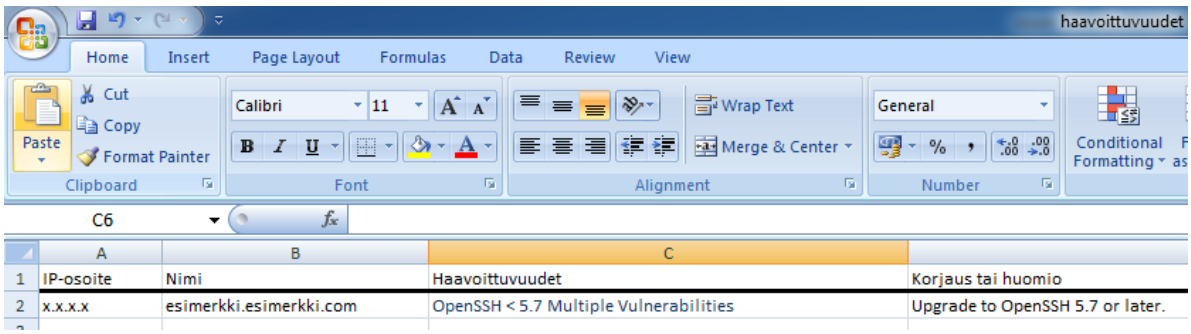
nmap –A <target-ip>

4.4.1 Exploittien etsiminen ja analysoiminen

Etsin eri tietokannoista sekä Googlen vapaa-sanahakua hyödyntämällä haavoittuvuuksia tietoturvakatsauksen kohteista. Esimerkiksi saatuani selville, että eräässä palvelimessa oli käytössä Apachen HTTPd-ohjelma ja sen versio oli 2.2.15, siirryin näiden tietojen perusteella etsimään Exploit DBstä exploittia, joita voisin sitten käyttää tunkeutumiseen toimeksiantajan järjestelmään. Löytämiäni haavoittuvuuksia yritin analysoida Internetistä löytämieni eri lähteiden tietojen perusteella.

4.4.2 Havainnoinneista raportoiminen

Listasin löytämäni haavoittuvuudet Excelillä. Siitä selviää kohteen IP-osoite, nimi, haavoittuvuus ja korjaustoimenpide, jos sellainen on olemassa. Raporttia ei kuitenkaan julkaista opinnäytetyössä tietoturvasyistä. Tämän opinnäytetyön havainnot osioissa on yleisesti kerrottu löydetyistä puutteista. Alla olevassa kuvassa esimerkki raportista:



Kuva 5. Esimerkki toimeksiantajalle toimitettavasta raportista.

5 HAVAINNOT JA KORJAUSEHDOTUKSET

Tietoturvakartoituksessa tutkin toimeksiantajan tietoverkkoa ja järjestelmiä sekä ulko- että sisäverkosta. Yritin löytää mahdollisimman paljon turhia avoimia portteja, päivittämättömiä palveluita ja niiden riskejä. Tutkiessani käytin hyväkseni esimerkiksi Nmap-ohjelmaa, Internetiä, saatavia dokumentaatioita ja konfiguraatioita. Ulkoverkosta tutkin palomuurin määrityksiä, isäntiä ja niiden palveluita. Lisäksi yritin havaita mahdollisimman laaja-alaisesti puutteita toimeksiantajan tietoturvan osalta liittyen teknologiaan. Yksi suurimmista yksittäisistä haavoittuvuusriskeistä oli käytössä ollut Windows 2003 Server. Seuraavissa alakappaleissa olen käynyt läpi omasta mielestäni huolestuttavimpia puutteita, joita havaitsin tietoturvakartoituksessa. Korjausehdotuksia laadin toimeksiantajalle sopivan laajuuden mukaan ja niin, etteivät muutoksiin käytettävät taloudelliset panostukset nousisi liian suuriksi.

5.1 Palvelimien ja laitteiden haavoittuvuudet

Palvelimien eri palveluista löytyi useita haavoittuvuuksia. Esimerkiksi toimeksiantajalla oli käytössään Apache HTTPd ohjelmisto kuudessa eri palvelimessa ja niiden versiot olivat todella vanhoja, esimerkiksi eräässä palvelimessa oli versio 2.2.12, joka on julkaistu 28. heinäkuuta 2009. Toimeksiantajan ”uusin” käytössä oleva versio oli 2.2.15, joka on julkaistu 5. maaliskuuta 2010. Käytössä olleisiin versioihin oli saatavilla paljon julkisia exploitteja. Haavoittuvuuksilta suojautumiseen ohjelmat tulisi päivittää välittömästi. Lisäksi monessa palvelimessa Apacheen löytyi myös muitakin haavoittuvuuksia, joihin korjaukseksi tarvitsisi päivitysten lisäksi tehdä konfiguraatioon muutoksia.

Haavoittuvuuksia löytyi seuraavista palveluista:

- Apache HTTPd
- Apache Tomcat
- PHP
- phpMyAdmin
- OpenSSH
- vsftpd
- Wordpress
- Bugzilla

5.2 Tunkeutumisen havaitseminen ja estäminen

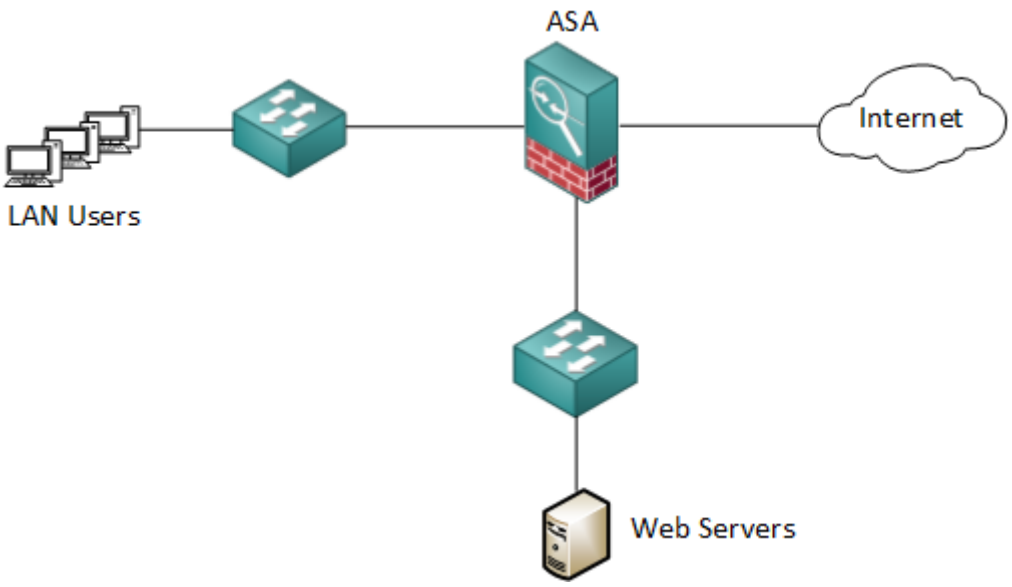
Toimeksiantajalla ei ollut käytössä minkäänlaista IDS tai IPS järjestelmää. Näin ollen toimeksiantaja ei pystynyt monitoroimaan ja seuraamaan mahdollisia tunkeutumisyrityksiä. IPS tai IDS olisi mahdollista toteuttaa erillisellä tietoverkkoon kytkettävällä laitteella tai Ciscon palomuurin liitettävällä lisäkortilla.

5.3 Palomuuri ja DMZ

Toimeksiantajalla oli käytössään Ciscon 5510 palomuurilaite, mutta sen konfiguraatio osoittautui puutteelliseksi ja osittain suunnittelemattomaksi. Palomuurinsäännöstö ei kaikilta osin ollut laadittu toimeksiantajan tarpeiden mukaan. Lisäksi kaikki palvelimet, joita tarjottiin käyttäjille, olivat palomuurin "samalla" puolella. Toimeksiantajan kaikkia palveluita ei kuitenkaan ole tarkoitus tarjota ulkoverkon suuntaan.

Palomuuri on tärkeimpien kriittisten tietoturvalaitteiden listalla, joita liiketoiminta käyttää suojellakseen omaisuuttaan, ja sen säännöt tulisi luoda niin, että liikenne sallitaan vain tarvittaville palveluille ja tarpeeton liikenne estetään. Organisaation omistaessa omat WWW-sivut, sähköpostin tai jonkin muun Internet-palvelun olisi syytä to-

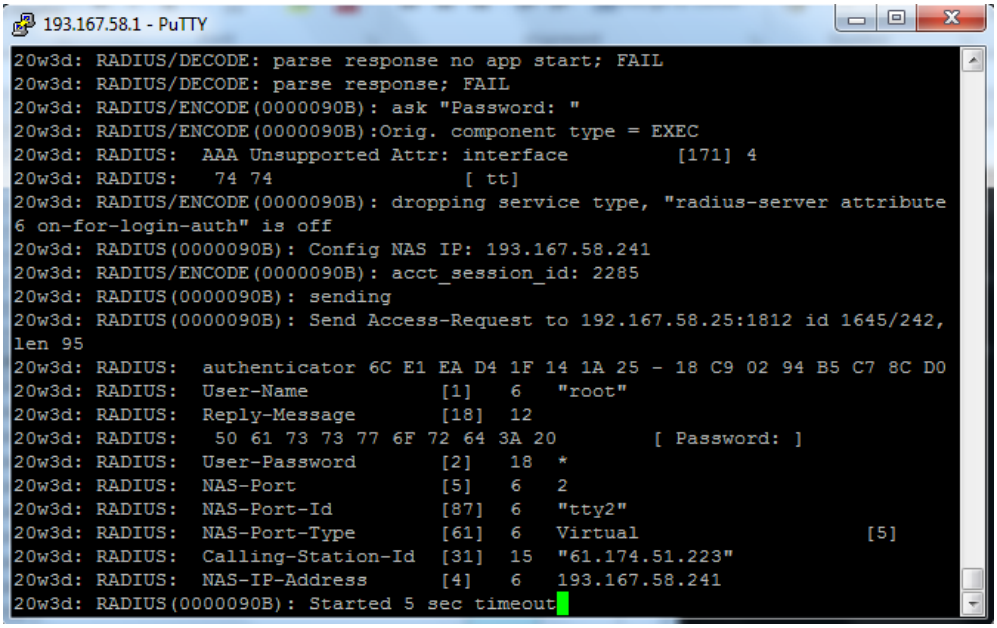
teuttaa palomuuri DMZ-ratkaisun kanssa. (Jackson 2010, 247, 249, 259.) Alla olevassa kuvassa ehdotus toimeksiantajalle:



Kuva 6. Ehdotus toimeksiantajalle palomuurista ja DMZ-ratkaisusta.

5.4 Etähallintayhteyksien rajoittaminen

Toimeksiantajan eri järjestelmien etähallintaan kirjautuminen onnistuu ulkoverkosta, eikä sitä ole juurikaan rajoitettu. Tästä hyvänä esimerkkinä Radiuksen debuggauksen ollessa päällä eräässä verkon aktiivilaitteessa havaitsin, että siihen yritetään kirjautua koko ajan. Omasta mielenkiinnostani selvitin lähdeosoitteen perusteella kirjautujan taustaa ja selvisi, että osoitteet johtavat Kiinaan ja osoitteiden haltijasta löytyi paljon negatiivista keskustelua. Alla olevasta kuvasta siis selviää, että laitteeseen yritettiin tunkeutua "root"-käyttäjätunnuksella ja salasanavaihtoehtoja käytiin läpi Bruteforce-tekniikalla.



Kuva 7. Tunkeutusmisyritys toimeksiantajan laitteeseen.

Toimeksiantajan olisikin syytä rajoittaa eri laitteiden etähallinta siten, että se onnistuisi vain sisäverkosta. Jos ulkoverkosta halutaan päästä etähallitsemaan, tulisi se toteuttaa niin, että ensiksi kirjauduttaisiin VPN-yhteydellä toimeksiantajan sisäverkkoon ja sieltä sitten itse etähallittavaan kohteeseen.

5.5 Lokitietojen hallinta

Keskusteltuani toimeksiantajan kanssa eri palveluiden ja laitteiden lokien hallinnasta ilmeni, ettei toimeksiantajalla ole käytössä minkäänlaista lokien hallintaa. Ilmeisesti erilaisista hälytyksistäkään ei tullut ilmoituksia toimeksiantajan henkilökunnalle. Lokien keskitetty hallinta helpottaisi järjestelmien monitorointia.

5.6 Lähiverkon aktiivilaitteet

Sisäverkosta tutkiessani verkon aktiivilaitteiden konfiguraatioita havaitsin, että aktiivilaitteiden käyttäjätunnukset ja salasana olivat liian helppoja ("well-known") ja salasanat olivat selkokielisinä laitteen konfiguraatiotiedostoissa. Osassa aktiivilaitteista oli myös määritetty sellaiset käyttäjätunnus−salasanayhdistelmät, joita ei kukaan toimeksiantajan henkilökunnasta tiennyt. Testasin yleisiä mahdollisia salasanoja tuloksetta. Mielestäni tämä oli myös hiukan huolestuttavaa, koska kukaan ei tiennyt, olisiko mahdollisesti tämä laite jonkin hallinnassa.

Aktiivilaitteiden etähallintaprotokollista oli käytössä HTTP ja TELNET, jotka pitäisi heti ottaa pois käytöstä. Ainoaksi etähallintaprotokollaksi tulisi ottaa käyttöön SSH. Tunnistautumisen voisi tehdä Radiuksen avulla SSH protokollaa käyttäen. Console-portin kautta puolestaan pääsisi laitteeseen käsiksi Radius-palvelimen ollessa alhaalla.

Verkon aktiivilaitteiden SNMP-community oli oletuksena, joka olisi myös syytä muuttaa joksikin vaikeammaksi. SNMP-yhteyksien ottaminen tulisi myös rajoittaa pääsylistalla siten, että se onnistuu vain hallinta-asemasta. Lisäksi mahdollisuuksien mukaan tulisi käyttää SNMP-versiota kolme.

Videovalvontajärjestelmän kamerat olivat samoissa virtuaalisissa lähiverkoissa kuin muutkin ja etenkin niiden julkinen IP-osoite vaikutti hiukan riskiltä. Lisäksi videovalvontajärjestelmään on mahdollista kirjautua ulkoverkosta suoraan.

6 YHTEENVETO

Kuten edellä luetellussa tietoturvakartoituksessa löytyneistä havainnoista käy ilmi, moniin haavoittuvuuksiin löytyi päivitys, joilla olisi saatu parannettua tietoturvan tasoa. Jatkuvasti julkaistaan uusia haavoittuvuuksia ja onkin tärkeää asentaa ohjelmistojen uusimmat päivitykset heti niiden julkaisun jälkeen. Palomuurin pitää olla suunniteltu pitämään suurin osa "pahasta" tiedosta verkon ulkopuolella, ja toimeksiantaja aloittikin välittömästi palomuurisäännöstön tiukentamisen.

Opinnäytetyöni tavoitteena oli toteuttaa tietoturvakatsaus Kymenlaakson ammattikorkeakoulun ICT-LAB:n tuotantoympäristöstä tietoturva-auditoinnin ja penetraatiotestauksen menetelmiä apuna käyttäen. Mielestäni onnistuin tavoitteeni saavuttamisessa pääosin hyvin, ja opinnäytetyöni pohjalta toimeksiantaja onkin toteuttanut muun muassa DMZ-alueen ja autentikointi on toteutettu Radiuksen avulla toisen opiskelijan opinnäytetyön toimeksiantona.

Tavoitteen saavuttamisen näkökulmasta teoriaosani jäsentyi melko hyvin. Mielestäni osasin rajata teoreettisen viitekehyksen opinnäytetyöni aiheeseen ja laajuteen nähden sopivaksi, vaikka käytännön osuutta toteuttaessani huomasinkin, että vieläkin tarkempi aiheen rajaus olisi ollut tarpeen. Pyrin kuitenkin huomioimaan teoriaosuudessani eri näkökulmat ja selostamaan ne riittävän kattavasti samalla yrittäen välttää liian laajaa teoreettista viitekehystä. Mielestäni onnistuin hankkimaan monipuolista ja hyvää läh-

dematerіaalia opinnäytetyöni teoriaosuuteen ja osasin rajata lähdemateriaalin olennaisimpaan.

Opinnäytetyöni käytännön osuuden edetessä ja kevään lähestyessä huomasin, että opinnäytetyöni aihe kokonaisuudessaan oli kuitenkin liian laaja suhteessa siihen käytettävissä oleviin resursseihin. Toisin sanoen aihepiiri oli monitahoinen ja näin ollen myös työn rajaus oli haastavaa ottaen huomioon opinnäytetyöni tavoitteen, jonka pohjalta opinnäytetyön aihetta tuli kuitenkin tarkastella melko laajasti riittävän pohjatiedon ja käytännön osuuden onnistumisen takaamiseksi. Mielestäni onnistuin hyvin jo edellä mainitussa pohjatiedon hankkimisessa ja teknologian tarkastelussa. Penetraatiotestauksessa ei ehditty hyväksikäyttövaiheeseen osittain runsaasti löytyneiden haavoittuvuuksien vuoksi ja lisäksi ajan loppuessa kesken. Opinnäytetyöni ei täysin saavuttanut sille asetettuja tavoitteita, mutta se toimii hyvänä pohjana Kymenlaakson ammattikorkeakoulun tuotantoympäristön tietoturvallisuuden parantamisessa. Jos aika ei olisi loppunut kesken, jatkaisin penetraatiotestausta hyödyntämällä löytämiäni haavoittuvuuksia.

Mielestäni yksi opinnäytetyön haastavimmista osuuksista oli varsinainen kirjoitusprosessi. Koska lähes kaikki lähdemateriaali oli englanninkielistä, kirjoittaminen vaati enemmän aikaa kuin olin ajatellut. Lisäksi asian merkityssisältöjen säilyttäminen oli haastavaa kääntäessäni tekstiä englannista suomen kielelle poimien samalla tärkeimmät asiat. Mielestäni onnistuin kuitenkin tässä melko hyvin.

Eettisyyden näkökulmasta pyrin ensiksikin kirjoittamaan koko opinnäytetyöni prosessin selkeästi ja avoimesti siten, kuin se oli mahdollista. Kuten jo aiemmin mainitsin, sovimme toimeksiantajan kanssa, ettei tarkkaa raporttia haavoittuvuuksista julkaista tässä työssä. Tämä tekijä osaltaan sekä lisää että heikentää opinnäytetyöni luotettavuutta, sillä raportin julkaisematta jättäminen lisää työn eettisyyttä estämällä hankitun tiedon hyväksikäyttämistä, mutta toisaalta saattaa heikentää sitä opinnäytetyöni luotettavuuden arvioinnissa. Toisekseen kaikki käytännön toteutukseen liittyvät toimenpiteet tein toimeksiantajan luvalla. Lisäksi mainittakoon, että hyvää eettistä käytäntöä noudattaen en tule myöskään itse käyttämään hyväkseni saamiani tietoja.

Opinnäytetyön aiheen saatuani olin hiukan epävarma, sillä aihealue ei ollut minulle entuudestaan kovinkaan tuttu. Täytyykin myöntää, että aihe oli osittain oman mukavuusalueeni ulkopuolella. Koulutuksemme aikana en ole saanut kovinkaan syvällisiä

valmiuksia aiheeseen liittyen, mutta mielestäni aiemmin koulutuksen puolesta hankittu tekninen osaaminen oli minulla hyvin hallussa, mikä hieman helpotti opinnäytetyön toteutuksen tekemistä. Koko opinnäytetyöprosessin ajan opin paljon uutta ja koen saaneeni paljon uusia taitoja. Osallistuminen Clarified Securityn järjestämään Hands on hacking -kurssiin kasvatti mielestäni valmiuksiani tehdä tämä opinnäytetyö laadukkaammin ja sen avulla omaksuin lisäksi sellaisen ajatusmallin, jota en muualta olisi saanut. Mielestäni koko opinnäytetyön prosessi kasvatti omaa asiantuntijuuttani aiheen näkökulmasta ja uskonkin, että opinnäytetyöstä on minulle joskus vielä hyötyä tulevaisuudessa.

Jatkotutkimusaiheina opiskelijat voisivat tehdä tietoturvakatsauksia jatkossakin, mutta he voisivat keskittyä johonkin tiettyyn osa-alueeseen yhdessä työssä. Yritin tehdä havaintoja mahdollisimman monilta osa-alueilta ja näin ollen puutteita jäi vielä varmasti huomaatta. Tulevaa kyberturvallisuuslaboratorioita ajatellen penetraatiotestaus tarjoaa varmasti tulevaisuudessa hyviä opinnäytetyön aiheita. ICT-LAB:n tuontantoympäristön kehittämisessä olisi varmasti monenlaisia kehittämismahdollisuuksia, esimerkkinä verkon topologian parantaminen, joita opiskelijat voisivat toteuttaa projektikursseilla tai kenties opinnäytetöissä.

LÄHTEET

Andersson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Tallinna: Tietosanoma Oy, s. 29, 51–52.

Engebretson, P. 2013. The basics of hacking and penetration testing. Waltham: Syngress, s. 1–2, 14, 20–23, 53–55, 85–86, 167–168.

Garfinkel, S. 2012. The Cybersecurity Risk. Communications of the ACM-lehti 1.6.2012, s. 29. Saatavissa: http://web.ebscohost.com.xhalax-ng.kyamk.fi:2048/ehost/pdfviewer/pdfviewer?sid=92d11621-bde3-4d9c-9d1e-234e81c38d9e%40sessionmgr14&vid=11&hid=28 [viitattu 12.11.2013].

Kyamk tietoverkkotekniikka. 2013. Kyberturvallisuus. Kyamk tietoverkkotekniikan Internet-sivut. Saatavissa: http://www.ictlab.kyamk.fi/index.php/kyperturvallisuus-menu [viitattu 15.11.2013].

Jackson, C. 2010. Network Security Auditing. Indianapolis: Cisco Press, s. 5–6, 10, 19–25, 68, 76, 91–92, 96, 101, 116, 247, 249, 259.

Kali Linux Documentation. 2013. Kali Linux Hard Disk Install. Kali Linux Dokumentation Internet-sivut. Saatavissa: docs.kali.org/installation/kali-linux-hard-disk-install [viitattu 14.1.2014].

Kali Linux Documentation. 2013. What is Kali Linux ?. Kali Linux Dokumentation Internet-sivut. Saatavissa: docs.kali.org/introduction/what-is-kali-linux [viitattu 14.1.2014].

Kettunen, M. 2014. Informaatioteknologian tiimin uudet visiot ja kyberturvallisuuslaboratoriohanke. Kyamk tietoverkkotekniikan Internet-sivut. Saatavissa: http://cisco.ictlab.kyamk.fi/ictlab/Informaatioteknologia/koskinen_kyberturvallisuus_valmis.pdf [viitattu 4.3.2014].

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita Publishing Oy, s. 216.

Melnichuk, D. 2008. The Hacker´s Underground Handbook. s. 7, 47, 53, 58–59.

Pale, P. 2012. Nmap 6: Network Exploration and Security Auditing Cookbook. Birmingham: Packt Publishing Ltd, s. 10, 20.

Puolustusministeriö. 2011. Yhteiskunnan turvallisuusstrategia. Valtioneuvoston periaatepäätös 16.12.2010. s. 1-3. Vammala: Vammalan kirjapaino.

Turvallisuuskomitean sihteeristö. 2013. Suomen kyberturvallisuusstrategia. Valtioneuvoston periaatepäätös 24.1.2013. s. 1-2, 6. Forssa: Forssa print.

Wilhelm, T. 2013. Professional Penetration Testing. Waltham: Syngress, s. 151-158, 172, 211–213.